

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 84678	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416).	
International application No. PCT/AU99/00486	International filing date (<i>day/month/year</i>) 17 June 1999	Priority Date (<i>day/month/year</i>) 17 June 1998
International Patent Classification (IPC) or national classification and IPC Int. Cl. ⁷ A63F 5/04, 9/24		
Applicant ARISTOCRAT TECHNOLOGIES AUSTRALIA PTY LTD et al		

1.	This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.																
2.	<p>This REPORT consists of a total of 3 sheets, including this cover sheet.</p> <p><input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of 7 sheet(s).</p>																
3.	<p>This report contains indications relating to the following items:</p> <table border="0"> <tr> <td>I</td> <td><input checked="" type="checkbox"/> Basis of the report</td> </tr> <tr> <td>II</td> <td><input type="checkbox"/> Priority</td> </tr> <tr> <td>III</td> <td><input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</td> </tr> <tr> <td>IV</td> <td><input type="checkbox"/> Lack of unity of invention</td> </tr> <tr> <td>V</td> <td><input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</td> </tr> <tr> <td>VI</td> <td><input type="checkbox"/> Certain documents cited</td> </tr> <tr> <td>VII</td> <td><input type="checkbox"/> Certain defects in the international application</td> </tr> <tr> <td>VIII</td> <td><input type="checkbox"/> Certain observations on the international application</td> </tr> </table>	I	<input checked="" type="checkbox"/> Basis of the report	II	<input type="checkbox"/> Priority	III	<input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability	IV	<input type="checkbox"/> Lack of unity of invention	V	<input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement	VI	<input type="checkbox"/> Certain documents cited	VII	<input type="checkbox"/> Certain defects in the international application	VIII	<input type="checkbox"/> Certain observations on the international application
I	<input checked="" type="checkbox"/> Basis of the report																
II	<input type="checkbox"/> Priority																
III	<input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability																
IV	<input type="checkbox"/> Lack of unity of invention																
V	<input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement																
VI	<input type="checkbox"/> Certain documents cited																
VII	<input type="checkbox"/> Certain defects in the international application																
VIII	<input type="checkbox"/> Certain observations on the international application																

Date of submission of the demand 17 January 2000	Date of completion of the report 6 July 2000
Name and mailing address of the IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized Officer J.W. THOMSON Telephone No. (02) 6283 2214

I. Basis of the report

1. With regard to the **elements** of the international application:*
- ☐ the international application as originally filed.
- ☒ the description, pages 1 - 18, as originally filed,
pages , filed with the demand,
pages , received on with the letter of
- ☒ the claims, pages , as originally filed,
pages , as amended (together with any statement) under Article 19,
pages , filed with the demand,
pages 19 - 25, received on with the letter of 30 June 2000
- ☒ the drawings, pages 1 - 4, as originally filed,
pages , filed with the demand,
pages , received on with the letter of
- ☐ the sequence listing part of the description:
pages , as originally filed
pages , filed with the demand
pages , received on with the letter of
2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language which is:
- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, was on the basis of the sequence listing:
- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished
4. ☐ The amendments have resulted in the cancellation of:
- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/fig.
5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims 1 - 64	YES
	Claims	NO
Inventive step (IS)	Claims 1 - 64	YES
	Claims	NO
Industrial applicability (IA)	Claims 1 - 64	YES
	Claims	NO

2. Citations and explanations (Rule 70.7)

US 5707286

US 5643086

JP 10-024148

These citations do not disclose the invention as defined in claims 1 to 64.

CLAIMS:

1. A control system for use with an electronic gaming device, the control system comprising:

a control means in electronic communication with the gaming device,
the control means including:

a microprocessor means (a central processing unit ["CPU"]);

a memory means;

a storage means;

a means for operating the gaming device, the means for operating
being stored in the memory means;

the memory means and the storage means further including a plurality
of program means and a plurality of data means, and a method to verify the
integrity of the program means and the data means (the verification method);

a plurality of input/output means;

a means for receiving power; and

a means for supplying power to the control system, the means for
supplying power in electrical communication with the means for receiving
power.

2. The control system as described in Claim 1, wherein each program
means and each data means includes an identification means, such that each
program means and each data means is uniquely identified (an established
identification means).

3. The control system as described in Claim 2, wherein the control
means further comprise a means for controlling one or more peripheral
devices.

4. The control system as described in Claim 3, further comprising a
second means for controlling one or more peripheral devices, the second
means for controlling peripheral devices in communication with the control
means.

5. The control system as described in Claim 3, wherein the first means for
controlling peripheral devices is an Input/Output Control Board (IOCB).

6. The control system as described in Claim 5, further comprising a
means for storing non-volatile memory.

7. The control system as described in Claim 6, wherein the storage means
is chosen from the group consisting of a ROM, PROM, EPROM or EEPROM.

8. The control system as described in Claim 7, wherein the verification

method further includes a method for grouping the program means that are related, and for grouping the data means that are related the method for grouping emulating a method of grouping employed in storage media.

9. The control system as described in Claim 8, wherein the storage media
5 whose grouping method is emulated is chosen from the group of storage media consisting of ROM, PROM, EPROM or EEPROM.

10. The control system as described in Claim 9, wherein the verification method further includes a method of abstracting the location of the program means, the data means and the storage means.

10 11. The control system as described in Claim 10, wherein the verification method, further includes means to compare the identification means of the requested program means or of the requested data means to the established identification means.

12. The control system as described in Claim 11, wherein the verification
15 method further includes a method of controlling the operation of the gaming device in response to the verification of integrity of the program means or the data means.

13. The control system as described in Claim 12, wherein the controlling method includes a means of halting the verification method if the
20 identification means of the requested program means or the requested data means does not match the established identification means of the program means or the data means.

14. The control system as described in Claim 13, wherein the verification method further includes a method to authenticate the retrieved program
25 means or the retrieved data means.

15. The control system as described in Claim 14, wherein the control means effects the method to authenticate only after the integrity of the requested program means or the integrity of the requested data means has been verified.

30 16. The control system as described in Claim 1, wherein the method to verify the integrity of the program means and the data means further includes a method to authenticate the program means and the data means, the authentication method being activated in response to signals received from a requesting means.

35 17. The control system as described in Claim 15, wherein the requesting means is an authentication agent.

18. The control system as described in Claim 16, wherein the authentication agent is external to the control system and the gaming device, the authentication agent in communication with the control means.

19. The control system as described in Claim 16, wherein an authentication agent is external to the control system and is within the gaming device, the authentication agent in communication with the control means.

20. The control system as described in Claim 17 or Claim 18, wherein the authentication method further includes a method for registering the authentication agents.

21. The control system as described in Claim 18, wherein the signal received from the requesting means is an authentication request.

22. The control system as described in Claim 1, wherein the control means further includes a means for receiving the authentication requests.

23. The control system as described in Claim 1, wherein the authentication requests includes a signal to prioritize the authentication request.

24. The control system as described in Claim 23, wherein the control means further includes a method to queue the authentication requests, when more than one authentication request has been sent from the authentication agents.

25. The control system as described in Claim 24, wherein the control means further include a means of interpreting the authentication request.

26. The control system as described in Claim 25, wherein the means of interpreting the authentication request includes a means of generating an authentication identification (id) of the requested program means or data means.

27. The control system as described in Claim 26, wherein the control system further includes a responder means, the responder means being external to the control means and in electronic communication with the control means.

28. The control system as described in Claim 27, wherein the control means further includes a presenter means, the presenter means communicating the generated authentication id to the responder means.

29. The control system as described in Claim 28, wherein the control means and the responder means include a method of determining if the

generated authentication id is authentic, the responder means comparing the generated authentication id to the request, the generated authentication id deemed authentic if the generated authentication id matches the request.

5 30. The control system as described in Claim 29, wherein the generated authentication id is deemed not authentic if the generated authentication id does not match the request.

31. The control system as described in Claim 29 and 30, wherein the control means further includes a means of controlling the operation of the gaming device in response to the determination of authenticity of the
10 requested program means or the requested data means.

32. The control system as described in Claim 31, wherein the controlling means includes means of halting the operation of the gaming device if the requested program means or the requested data means is deemed not authentic.

15 33. The control system as described in Claim 31, wherein the controlling means includes means of continuing the operation of the gaming device if the requested program means or the requested data means is deemed authentic.

20 34. The control system as described in Claim 9, wherein the storage means is a hard disk drive unit.

35. The control system as described in Claim 9, wherein the storage means is a CD-ROM unit.

36. The control system as described in Claim 9, wherein the storage means is a DVD unit.

25 37. The control system as described in Claim 9, wherein the storage means is a file server.

38. For use in an electronic gaming device, a method to verify the integrity of program means and the integrity of data means stored in a control system, the control system comprising:

30 a control means in electronic communication with the gaming device, the control system including;

a microprocessor means (a central processing unit ["CPU"]);

a memory means;

a storage means;

35 a means for operating the gaming device, the means for operating being stored in the memory means;

RECEIVED BY
ART 34 AMDT

the memory means and the storage means further including a plurality of program means and a plurality of data means. each program means and each data means having an identification means, such that each program means and each data means is uniquely identified (an established
5 identification means);

a plurality of input/output means;

a means for receiving power; and

a means for supplying power to the control system, the means for
supplying power in electrical communication with the means for receiving
10 power, the verification method comprising the steps of:

sending a request from a requesting means to the control system;

processing the request within the control system;

retrieving a requested program means or a requested data means from
the storage means;

15 verifying the integrity of the requested program means or the
requested data means by verification means which verify by comparing the
identification means of the requested program means or the requested data
means with the request, the integrity verified if the identification means
matches the established identification means request; and

20 controlling the operation of the gaming device in response to the
verification of integrity of the requested program means or the requested data
means.

39. The method as described in Claim 39, further comprising the steps of
halting the verification method of the identification means of the requested
25 program means or the requested data means does not match the established
identification means of the program means or the data means.

40. The method as described in Claim 39, further comprising a method to
authenticate the retrieved program means or the retrieved data means.

41. The method as described in Claim 40, wherein the method to
30 authenticate is effected only after the integrity of the requested program
means or the integrity of the requested data means has been verified.

42. The method as described in Claim 41, wherein the requesting means is
an authentication agent.

43. The method as described in Claim 42, wherein the method further
35 includes a method for registering the authentication agent.

44. The method as described in Claim 43, wherein the request includes a

verification request and an authentication request.

45. The method as described in Claim 44, wherein the request further includes an authentication queuing request.

5

46. The method as described in Claim 45, wherein the request further includes registration means for the authentication agent.

47. The method as described in Claim 43, further including a method of abstracting the location of the program means, the data means, and the storage means.

10

48. The method as described in Claim 47, further including the step determining which of the program means are related, and determining which of the data means are related.

49. The method as described in Claim 48, further including the step of grouping the related program means, and grouping the related data means.

15

50. The method as described in Claim 49, wherein the grouping step emulates a method of grouping employed in storage media chosen from the group consisting of ROM, PROM, EPROM or EEPROM.

51. The authentication method as described in Claim 50, wherein the control means further includes a means for queuing the authentication requests.

20

52. The authentication method as described in Claim 51, further comprising the step of queuing the authentication requests, when more than one authentication request has been sent from the authentication agents.

53. The authentication method as described in Claim 52, wherein the control means further includes a means of interpreting the authentication request.

25

54. The authentication method as described in Claim 53, further comprising the step of interpreting the authentication request.

55. The authentication method as described in Claim 54, wherein the interpretation step includes the step of generating an authentication identification (id).

30

56. The authentication method as described in Claim 55, wherein the control means further includes a presenter means, the presenter means communicating the generated authentication id to a responder means.

57. The authenticating method as described in Claim 56, further comprising the step of determining if the generated authentication id is authentic, the responder means and the control means comparing the

35

generated authentication id to the request, the generated authentication id deemed authentic if the generated authentication id matches the request.

58. The authentication method as described in Claim 57, wherein the generated authentication id is deemed not authentic if the generated authentication id does not match the request.

59. The authentication method as described in Claim 57 or 58, further including the step of controlling the operation of the gaming device in response to the determination of authenticity of the requested program means or the requested data means.

60. The method as described in Claim 59, wherein the controlling step includes halting the operation of the gaming device if the requested program means or the requested data means is determined to be not authentic.

61. The method as described in Claim 59, wherein the controlling step includes continuing the operation of the gaming device if the requested program means or the requested data means is determined to be authentic.